ENCRYPTION/DECRYPTION INSTRUCTION SET ENHANCEMENT

Don Van Dyke
Korbin Van Dyke
Stephen C. Purcell

ABSTRACT

A structure and associated method to implement encryption/decryption under the Data Encryption Standard (DES). Several additional instructions are included in the instruction set of a general purpose microprocessor to operate in conjunction with hardware included in a data path of the general purpose microprocessor. The additional instructions perform a portion of the DES algorithm, in particular, a portion of a DES round. The state information used at each step of the encryption portion of the DES algorithm is provided in various general purpose registers of the general purpose microprocessor. In one embodiment, all sixteen subkeys are selected prior to the DES step in the general processor after a DES key is known. In another embodiment, each subkey is selected during the round it is used. In yet another embodiment, each subkey is selected during the round it is used, as part of an additional instruction executed by the general purpose microprocessor.